REMARKS

Claims 1 through 30 are pending in the above-identified patent application. Claims 1 through 30 were rejected in the Office Action dated October 4, 2003.

Objections to the Drawings

In section 1 of the Office Action, the Examiner objected to the drawings for the reasons stated in PTO-948. The informalities are being corrected with replacement drawings submitted herewith. Accordingly, Applicant requests withdrawal of this objection.

Rejections Under 35 U.S.C. §112

In section 2 of the Office Action, the Examiner rejected claims 19 and 20 under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps. Specifically, the Examiner states that the step of deriving a key is missing and that there is no end result. Applicant traverses this rejection.

Claims 19 and 20 are implemented by a server that does not do decryption in this case. The decryption is handled by the client, as is recited in other claims, and therefore is not relevant to these claims. Accordingly, Applicant request withdrawal of this rejection.

Rejections Under 35 U.S.C. §102

In section 3 of the Office Action, the Examiner rejected claims 1 – 18 and 21 – 30 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,491,752 to Kaufman et al. (hereinafter *Kaufman*). Applicant traverses this rejection.

Claim 1, as amended, is patentable over *Kaufman* by at least reciting:

A <u>client-based</u> method, comprising:
      obtaining a hint;
      obtaining a password;
      performing a hashing algorithm on the hint and the password to generate a key;
      encrypting data using the key; and
      sending the encrypted data to a server for storage.

In contrast, *Kaufman* discloses a workstation (e.g., client) obtaining a token and password, hashing the token and password into a transmission code, and then transmitting the

transmission code to a server (Column 7, lines 1 – 5). The server then attempts to duplicate the transmission code by hashing tokens obtained by the server that might correspond with the token obtained by the workstation with passwords from a password list (Column 7, lines 6 – 14). If the server-generated transmission code matches the workstation transmission code, then a workstation user is granted access to desired computing services (Column 7, lines 15 – 18).

In comparison, the method as recited in claim 1 hashes a hint and password to encrypt data and then transmits the encrypted data to the server for storage. The method of claim 1 does not transmit the hashed hint and password as recited in *Kaufman* and even if it did, the purpose as claimed is for storage of data and not for granting access to computing services. Accordingly, claim 1 is patentable over *Kaufman*. Further, claims 2 and 3 should be patentable because of their dependency. In addition, claims 4 – 10 should be patentable because they recite substantially similar limitations to claim 1 and its dependent claims. Therefore, Applicant request withdrawal of the rejection of claims 1 – 10.

Claim 11 is patentable over *Kaufman* by at least reciting:

A method, comprising:
    receiving a request to store encrypted data from a client;
    sending an encryption downloadable for deriving a key to encrypt data to the client;
    receiving encrypted data that was encrypted by the encryption downloadable from the client; and
    obtaining a hint, corresponding to the encrypted data and needed for regenerating the key; and
    storing the hint and the encrypted data.

In contrast, *Kaufman* does not teach receiving a request to store encrypted data. As mentioned above, *Kaufman* teaches granting access to computing services. Further, *Kaufman* does not teach sending an encryption downloadable for deriving a key to encrypt data to the client. *Kaufman* instead teaches transmitting an encrypted message and challenge to a client. Accordingly, as *Kaufman* does not teach transmitting the downloadable, *Kaufman* cannot teach (and does not teach) receiving encrypted data encrypted by the downloadable from the client. Instead, *Kaufman* teaches decrypting the encrypted message sent by the server. Therefore, claim 11 is patentable over *Kaufman* as is claim 12, which recites similar limitations.

Claim 13 is patentable over *Kaufman* by at least reciting:

A <u>client-based</u> method, comprising:
obtaining a password;
receiving encrypted data and a hint corresponding to the encrypted data
from a server; and
performing a hashing algorithm on the password and the hint to generate a
key for decrypting the encrypted data.

In contrast, *Kaufman* teaches sending encrypted data to a workstation but does not teach

sending a hint to the workstation (and therefore receiving a hint from a server) as recited in claim

13 (Figure 6 and associated text). Accordingly, claim 13, and therefore its dependent claim in

addition, are patentable over *Kaufman*. Further, claim 15, 16 and its dependent claims are

patentable over *Kaufman* as they recite similar limitations.

Claim 21 is patentable over *Kaufman* by at least reciting:

A client-based method, comprising:
obtaining a password;
deriving a first secret from the password;
receiving a hint corresponding to data to be decrypted from a server;
deriving an intermediate index from the first secret and the hint; and
sending the intermediate index to the server.

In contrast, *Kaufman* does not teach deriving a first secret from the password but instead

teaches hashing (i.e., encrypting, which is the opposite of deriving) the password and token

(Column 9, line 40 – Column 10, line 17). Further, *Kaufman* does not disclose receiving a hint

from a server. *Kaufman* only teaches sending encrypted data to the client (FIG. 6). Accordingly,

claim 21 and dependent claims are patentable over *Kaufman*. Further, claim 26 and its

dependent claims should be patentable over *Kaufman* since they recite similar limitations.

Claim 24 is patentable over *Kaufman* by at least reciting:

A system, comprising:
a user interface for obtaining a password;
an index generator coupled to the user interface for generating an
intermediate index from a hint received from a server and a secret derived from
the password; and
a communications engine coupled to the index generator for sending the
intermediate index to the server.

In comparison, *Kaufman* does not teach receiving a hint from a server. Only encrypted

data is sent from the server to a workstation (FIG. 6 and associated text). Accordingly, claim 24

is patentable over *Kaufman*. Further, claim 25 should be patentable over *Kaufman* at least due to its dependency.

Claim 29 is patentable over *Kaufman* by at least reciting:

A server-based method, comprising:
   receiving an indication of encrypted data to be decrypted;
   transmitting to a client a hint corresponding to the indication, and a
decryption downloadable for deriving an intermediate index from a password and
the hint;
   receiving the intermediate index from the client; and
   deriving a decryption key from a second secret corresponding to the user
and the intermediate index.

In contrast, *Kaufman* does not teach sending to the client a hint. *Kaufman* only teaches transmitting encrypted data to the client (FIG. 6 and associated text). Accordingly, claim 29 is patentable over *Kaufman*.

Claim 30 is patentable over *Kaufman* by at least reciting:

A system, comprising:
   a second secret corresponding to a user;
   a decryption downloadable for generating an intermediate index from a
password and a hint;
   a web server for receiving an indication of encrypted data to be decrypted,
for transmitting the decryption downloadable and a hint corresponding to the
indication to a client, and for receiving an intermediate index from the client; and
   a server-resident module for deriving a key for decrypting the encrypted
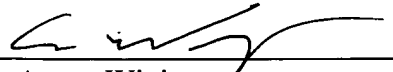data from the second secret and the intermediate index.

In contrast, *Kaufman* does not teach a decryption downloadable or transmitting the decryption downloadable and hint to a client. In actuality, *Kaufman* discloses that the client decrypts an encrypted message (FIG. 6 and associated text) received from the server and also encrypts data to from a transmission code (Column 7, lines 2 – 5). Therefore, claim 30 is patentable over *Kaufman*.

As all §102 rejections have been overcome, Applicant respectfully requests withdrawal of this rejection. Further as only patentable claims are present, Applicant requests a Notice of Allowance be timely issued.

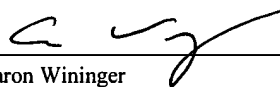If the Examiner has any questions, he is invited to contact the undersigned at 1.650.843.3375.

Respectfully submitted,
Mark D. Riggins

Dated: _/ 2 /1/o3_   By _____
Squire, Sanders & Dempsey L.L.P.   Aaron Wininger
600 Hansen Way   Attorney for Applicants
Palo Alto, CA 94304-1043   Reg. No. 45,229
Telephone (650) 856-6500
Facsimile (650) 843-8777

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being
attached or enclosed) is being deposited with the United States Postal
Service on the date shown below with sufficient postage as first class
mail in an envelope addressed to Mail Stop Non-Fee Amendment,
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-
1450, on

Date: _/2/1/93_ By: _____
                      Aaron Wininger